TELECOPIER TRANSMISSION
TO THE UNITED STATES PATENT AND TRADEMARK OFFICE

(703) 872-9306

TO: EXAMINER Cristina O. Sherr

EXAMINER'S TELEPHONE NUMBER 571-272-6711

ART UNIT 3621

SERIAL NO. 09/454,349

FROM: Edward W. Goodman

REGISTRATION NO. 28,613

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510-8001
TELEPHONE: 914-333-9611
FACSIMILE: 914-332-0615

Enclosed: R116 Response + Cover

I certify that this document consisting of 8 pages (including this cover sheet) is being transmitted via telecopier to the United States Patent and Trademark Office at the telephone number set forth above on April 29, 2005.

Edward W. Goodman

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Atty. Docket

MICHAEL A. EPSTEIN PHA 23,637

Serial No.: 09/454,349 Group Art Unit: 3621

Filed: December 3, 1999 Examiner: C.O. Sherr

Title: DEY DISTRIBUTION VIA A MEMORY DEVICE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Enclosed is an amendment in the above-identified application.

[X] No additional fee is required.

[ ] The fee has been calculated as shown below.

CLAIMS AS AMENDED				
	Claims remaining after amendment	Highest number previously paid for	Number extra Rate	Additional Fee
Total Claims	20 Minus	20 [1] =	X $50 =	$
Independent Claims	5 Minus	5 [2] =	X $200 =	$
Multiple Dependent Claims, if any. If not previously paid, $360.				$
Total Additional fee for this amendment =				$

[1] If less than 20, enter 20. [2] If less than 3, enter 3.

Please charge any fees which may be required, except the issue fee, or credit any overpayment to Deposit Account No. 14-1270.

Edward W. Goodman, Reg. 28,613
914-333-9611

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of
MICHAEL A. EPSTEIN
SERIAL NO.: 09/454,349
FILED: December 3, 1999
KEY DISTRIBUTION VIA A MEMORY DEVICE

Atty. Docket
PHA 23,637
GROUP ART UNIT: 3621
EXAMINER: C.O. Sherr

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

RESPONSE UNDER 37 C.F.R. 1.116

This is in response to the Office Action mailed March 31, 2005, in which the Examiner finally rejected claims 1-20 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patetn 5,857,021 to Kataoka et al.

Applicant traverses the above rejection and offers the following explanation.

The Kataoka et al. patent discloses a security system for protecting information stored in portable storage media in which a medium ID, a corporate ID and a terminal ID are used to protect the use of content material. In a particular embodiment described at col. 6, line 51 to col. 7, line 25, a first private key generating means 105 generates a private key, based on a medium ID 121 extracted from the storage medium and a unit ID 104 (e.g., a unique identifier of the computer system or of a portable drive unit. A

first encrypting means 107 encrypts a data encryption key 106 with the private key, and the encrypted data encryption key is written into the storage medium. A second encrypting means 108 encrypts the data to be stored with the data encryption key, and the encrypted data is written into the storage medium.

In the subject invention, as claimed in, for example, claims 1, content material is encrypted using an encryption code. The encrypted content material is then written into a recording medium in a first writing operation. The recording medium includes a recording indicator which, in response to the first writing operation, generates and stores a unique identifier. This unique identifier is used with the encryption code to form a secure item which is then written into the recording medium in a second writing operation.

The Examiner now states "Although the cited art does not specifically claim such a unique identifier being generated by the first write operation, Kataoke does discloses encrypting data through known algorithms or key generating means (e.g. col 7, ln 5-10, col 5 ln 15-20). Thus steps need only be shuffled, reordered or repeated more time in order to obtain a unique identifier. Mere reordering or repeating of steps at different stages does not constitute new art."

Applicant submits that the Examiner has missed an important feature of the subject invention. In particular, the

Kataoka et al. data encoding system, shown in Fig. 9 therein, is described at col. 7, lines 10-26:

> "The first private key generating means 105 generates a private key, based on the medium ID 121 extracted from the storage medium 101 and a unit ID 104. The unit ID 104 is a unique identifier of the computer system itself or that of a portable drive unit (e.g., an MO drive). While the former identifier is normally used as the unit ID 104, the latter may be useful in some situations such as system installation or maintenance, because it is possible to install programs, set up data, and modify data using the same drive unit and storage medium for different computer systems. The first encrypting means 107 encrypts the data encryption key 106 with the private key generated by the first private key generating means 105. The encrypted encryption key is written into the storage medium 101 as the aforementioned permission data 122. The second encrypting means 108 encrypts the data with the data encryption key 106 and writes the encrypted data into the storage medium 101 as the aforementioned encrypted data 123."

Superficially, this may appear to be the same as the subject invention. However, it should be noted that the medium ID 121 "is an identifier uniquely assigned to the storage medium 101, which is burned into a predetermined region in a non-rewritable manner with a laser beam, for example" (col. 6, lines 64-67). As such, no matter how many different times encrypted data is to be stored on the storage medium 101, the same medium ID 121 is used to encrypt the encryption key for storage on the storage medium 101.

In the subject invention, on the other hand, a recording medium comprises "a recording indicator for generating and storing a unique identifier at each occurrence of the first write operation". As described in the Substitute Specification on page 8,

paragraph [0014], "A new number U (unique identifier) is created each time encrypted content material 221 is stored to the memory area 320 of the medium 300." Hence, the recording medium contains a, for example, number generator for generating and storing a new unique identifier each time encrypted content material is stored in a first memory of the recording medium via a first write operation. The content provider 200 then receives this unique identifier and the unique identifier to encrypt the encryption key used to encrypt the encrypted content material. This encrypted encryption key (secure item) is then written into a second memory of the recording medium via a second write operation.

Applicant submits that Kataoka et al. teaches away from the subject invention in that Kataoka et al. goes to great lengths to make sure that the medium ID is unchangeable, while, in the subject invention, the unique identifier changes for each first write operation.

It appears that the Examiner dismisses this feature by indicating that Kataoka et al. "discloses encrypting data through known algorithms or key generating means", and then stating that mere reordering or repeating of steps at different stages does not constitute new art. However, Applicant submits that the subject invention does not merely reorder or repeat steps taken by Kataoka et al. at different stages. Rather, the subject invention adds a new level of security.

Applicant understands that there are numerous different algorithms which can be used for encryption, and Applicant is not trying to come up with a new algorithm for encrypting the content material, or for encrypting the encryption key used to encrypt the content material. Nor is Applicant trying to come up with an additional key generator to be used in the content provider 200 (i.e., recording device). Rather, Applicant has found that an added level of security is achieved when the **recording medium** comprises "a recording indicator for generating and storing a unique identifier at each occurrence of the first write operation" (i.e., the storing of encrypted content material in a first memory of the recording medium), this unique identifier being used to form a secure item which is stored in a second memory of the recording medium via a second write operation when the encrypted content material is stored.

In view of the above, Applicant believes that the subject invention, as claimed, is not rendered obvious by Kataoka et al., and as such, is patentable thereover.

Applicant believes that this application, containing claims 1-20, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by
Edward W. Goodman, Reg. 28,613
Attorney
Tel.: 914-333-9611